

## Course S Week 2

### Incident Response Overview

#### Events :

An event can be something as benign and remarkable as typing a keyword or receiving an email. In some cases if there is an IDS, the alert can be considered an even until validated as a threat.

#### Incidents

An incident is an event that negatively affects IT systems and impacts on the business. It's an

Incident -

Unplanned interruption or reduction  
in quality of an IT service.

An event can lead to an incident,  
but not the other way around.

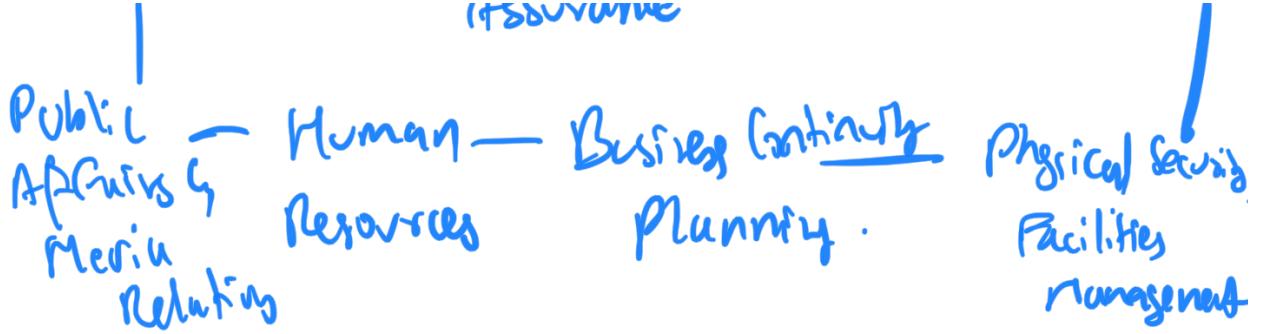
IR Team Models:

Central) — Distributed — Coordinating

Coordinating Teams

↳ Incidents don't occur in a vacuum  
can have an impact on multiple  
parts of a business · Establish  
relationships with the following  
teams:

Management (→ Information → IT Support — Log



## Common Attack Vectors :-

Organization should be generally prepared to handle any incident but should focus on being prepared to handle incidents that use common attack vectors.

1.) External / Removable Media

2.) Attrition

3.) Web

4.) Email

5.) Impersonation

6.) Loss - Talk - Environment.

or loss or theft of equipment.

## Incident Response Process.

### Incident Response Policy.

#### IR Team

The composition of the incident response team within the organization.

#### Roles

↳ The role of each of the team members.

#### Means, Tools, Resources.

→ The technological means, tools, and resources used.

unrecoverable that you need  
to identify and recover compromised  
data.

## Policy Testing

The person responsible for  
testing the policy.

## Action Plan

↳ How to put the policy  
into action.

The Best Offense, Risk Assessment,  
Host Security, Network security,  
Malware Prevention & User Awareness  
and Training.

Incident Response Detection & Analysis

Precursors is a sign that an incident may occur in future.

Indicators  $\Rightarrow$  A sign that an incident may have occurred or may be occurring now.

## Monitoring Systems:

$\hookrightarrow$  Monitoring systems are crucial for early detection of threats

$\hookrightarrow$  These systems are not mutually exclusive and still require IFR team to document and analyze the data

## Documentation

- 1.) The current status of the incident  
 $\hookrightarrow$  A summary of the incident

- 2.) ID summary of ...
- 3.) Indicators related to the incident
- 4.) Other incidents related to this incident.
- 5.) Actions taken by all incident handlers on this incident.

Incident Response Containment,  
Eradication, & Recovery.

Containment - An essential part of containment is decision making + such decisions are much easier to make if there are predetermined strategies and procedures for containing the incident

i.) Potential Damage to and

- 1) "theft of resources"
- 2) Need for evidence preservation
- 3) Service Availability
- 4) Time & Resources needed to implement the strategy
- 5) Effectiveness of the strategy.
- 6) Duration of the solution.

## Forensics in Incident Response .

- 1.) Capture a backup image of the system as-is
- 2.) Gather Evidence -
- 3.) Follow Chain of Custody protocols-

## Post Incident Activities.

→ Utilizing data collected,  
Evidence Retention  
Documentation

## Incident Response Demo

Common Threats → Software Attack  
Data Exfiltration  
Information sabotage  
Theft of Equipment

Attack Vectors → Website Hosting  
malicious content.  
These are typically  
Counteracted by the  
" "

following tools.

→ Qradar

→ McAfee ePolicy

Orchestrator

→ Next Generation  
Firewalls.

IR Process → Preparation  
Detection & Analysis  
Containment, Eradication,  
& Recovery.  
Post-Incident Activity